Instruction
Defense Intelligence Agency

DEFENSE INTELLIGENCE AGENCY
WASHINGTON, DC 20340-5100

DIAI 5400.001
8 March 2006
OPR: [redacted] (b)(3):10 USC 424

# Defense Intelligence Agency Privacy Act Program

**REFERENCES:**

(a) DIAR 12-12, "Defense Intelligence Agency Privacy Program", 15 April 1997 (cancelled)
(b) Title 5, United States Code, Section 552a, "The Privacy Act of 1974", (as amended)
(c) Title 5, United States Code, Section 552, as amended, "Freedom of Information Act"
(d) DoD Directive 5400.11, "Department of Defense Privacy Program", 16 November 2004
(e) DoD 5400.11-R, Department of Defense Privacy Program", August 1983
Additional references found at enclosure 1.

## 1. Purpose

1.1. Replaces reference (a).

1.2. This instruction implements references (b), (c), (d), (e) and (f) and establishes the Defense Intelligence Agency's (DIA) Privacy Act Program.

1.3. The DIA Privacy Act Program ensures the personal privacy of all individuals is respected and protected. It ensures personally identifiable information (PII) collected, maintained, used or disclosed by the Agency is relevant and necessary to accomplish the mission.

1.4. This instruction applies to all personnel employed by, assigned to, or attached for duty to the DIA; all DIA contractors and consultants; and all information processed, produced, used or stored by the DIA pertaining to these individuals. It provides procedures for the release of information maintained in records within the DIA.

## 2. Definitions (Terms of Reference) – see enclosure 2

## 3. Responsibilities

3.1. **The Director of DIA** has overall responsibility for ensuring compliance with the Privacy Act of 1974 (as amended).

3.2. **The Chief Privacy Officer (CPO).**

3.2.1. The CPO position was established to meet the concerns expressed in the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458) regarding the protection of privacy and civil liberties. The incumbent is responsible for ensuring the Agency is in compliance with applicable public law, as well as Office of the Director of National Intelligence, Office of Management and Budget, and Department of Defense (DOD) directives. Within DIA, the Vice Deputy Director for Administration (VDA) has been designated as the CPO by the Chief of Staff.

3.2.2. The CPO exercises general oversight of the Agency's privacy program and Privacy Act staff; ensures there is a valid and legal requirement for the collection of personal data; and provides direction and guidance for compliance with requirements of the Privacy Act of 1974 (as amended) in order to optimize the performance of the Agency and strengthen it as an institution.

3.2.3. The CPO serves as the Chairperson of the DIA Privacy Senior Steering Group.

3.2.4 The CPO reviews Section D (Privacy Section) of the Federal Information Management Act (FISMA) annual report, which provides guidance to the Privacy Act staff on the requirements which must be met to achieve compliance.

**3.3 DIA Privacy Senior Steering Group (Group).** The Group is comprised of senior executives representing the functional disciplines of the Agency (Collections, Analysis, Information Technology, Finance and Administration). The Group serves as the DIA Executive Committee for Privacy Act issues; ensures the Agency is in full compliance with applicable public law, as well as Office of the Director of National Intelligence, Office of Management and Budget, and DOD policies and directives and will:

3.3.1. Provide direction and guidance for compliance with the requirements of the Privacy Act of 1974 (as amended).

3.3.2. Prepare an annual assessment of the Agency's Privacy Program to include its "state of health" as pertains to compliance and execution of governing directives.

3.3.3. On an annual basis identify policies and/or processes that may need to be reviewed, modified, or eliminated to ensure compliance with existing directives.

**3.4. Chief Information Officer (CIO).** Is responsible for ensuring all new or modified IT systems that collect, maintain, or disseminate information in identifiable form from or

about members of the public, and/or new electronic collections of information in identifiable form comply with Section 208 of the E-Government Act of 2002 and DOD guidance for conducting Privacy Impact Assessments.

**3.5. General Counsel (GC).** The GC is the principal point of contact for legal matters related to the Privacy Act and will review all System of Records Notices (SORN) and Privacy Impact Assessments (PIA's) for legal compliance.

**3.6. Deputy Directors for and Special Staff Offices.** Deputy Directors for and Special Staff Offices are responsible for implementing and adhering to Privacy Act-related instructions (including the registration all new System of Records; assisting the CIO staff when Privacy Impact Assessments are conducted; identifying privacy issues of concern to the CPO or privacy staff for action).

**3.7. DIA Employees.** Although the Director of DIA has overall responsibility for ensuring compliance with the Privacy Act of 1974 (as amended), all employees (civilian, military and contractor) have a role in privacy awareness, compliance with pertinent privacy laws and directives, and the protection of personally identifiable information. All personnel must be aware of permissible and impermissible actions regarding personal data; procedures to protect this information; and appropriate responses to the loss, theft, or compromise of information in DIA control.

## 4. Procedures

### 4.1. Requesting records.

4.1.1. Individuals whose personal information is maintained by DIA's systems of records have the right to request copies of those records, consistent with the Privacy Act and other applicable laws, policies and directives. Release of personal information under this instruction is not considered public release of information.

4.1.2. Requests for records must be made in writing. The request should include the first name, middle name or initial, surname, date of birth, and Social Security Number of the requestor. It should provide a description of the record and the system in which the record is located. The request must be sent to [redacted] (b)(3):10 USC 424 [redacted] The following address should be used:

(b)(3):10 USC 424

Defense Intelligence Agency
Attn: [redacted] (b)(3):10 USC 424
200 MacDill Blvd
Washington DC 20340

4.2. **System of Records Notices.**

4.2.1. A system of records notice must be prepared whenever a new system, database or group of records is created, which contains information that is retrievable by the name of an individual or by some identifying number, symbol or other identifying particular assigned to an individual. The information must pertain to U.S. citizens, as defined in the Privacy Act of 1974 (as amended).

4.2.2. The Deputy Director for or Special Staff Office creating or maintaining the system is responsible for preparing the System of Records Notice. The privacy staff will work with the proponent of the system, database or group of records in the preparation of a System of Records Notice in accordance with guidance provided by the Defense Privacy Officer (OSD/DPO) of the Office of the Secretary of Defense. The privacy staff is responsible for submitting the SORN to the OSD/DPO for review and posting to the Federal Register. A sample format is at enclosure 3.

4.3. **Privacy Impact Assessments.**

4.3.1. A Privacy Impact Assessment (PIA) will be conducted by the Chief Information Officer (CIO) staff whenever developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public (excluding DOD personnel) or when initiating a new electronic collection of information in identifiable form for ten or more members of the public (excluding DOD personnel).

4.3.2. PIA's are only required for IT systems or websites that have direct interface with the general public. Therefore this requirement would NOT apply to internal IT systems, databases or websites which are only accessed by DOD employees (civilian, military or contractors).

4.3.3. Guidance, procedures and policy for conducting PIA's is maintained by the CIO staff.

4.3.4. The Chief Privacy Officer must coordinate on all PIA's before they are forwarded to the CIO for approval.

4.4. **Notifying individuals when personal information is lost, stolen, or compromised.**

4.4.1. In the event that personal information maintained by the Agency is lost, stolen or compromised; the Agency is committed to informing the workforce of the situation.

4.4.2. At a minimum the CPO will advise affected individuals of the specific data lost, stolen, or compromised; the circumstances surrounding the incident; and protective actions the individuals should take. Notifications to affected individuals will be made as soon as possible, but no later than ten days after the loss or compromise has been discovered. If affected individuals cannot be readily identified, DIA will provide a generalized notice to the potentially affected population.

4.4.3. Personnel notified of actual loss or potential compromise should take action based on guidance provided on the Federal Trade Commission's website, www.consumer.gov/idtheft. This site offers helpful information and guidelines to follow to avoid becoming a victim of identity theft.

(b)(3):10 USC 424

4.4.4. Individuals becoming aware of the possible loss, theft, or compromise of personal information should notify the DIA Privacy Office via email or phone immediately. Information to be reported includes description of the lost, stolen, or compromised information, the database/system which contained the information, when the suspected loss, theft, or compromise occurred, and any other relevant information in the individual's possession.

(b)(3):10 USC 424

(b)(3):10 USC 424

## 4.5. **Protection of Privacy Data.**

4.5.1. All systems of records containing PII will be properly protected IAW with established Privacy Act standards to ensure access is limited to those having a need to know in the performance of their assigned duties.

4.5.2. File folders containing PII must have Optional Form 86, Personal Data label affixed to them. File cabinets used to store PII must be secured and access to them limited.

4.5.3. File plans will identify files which contain privacy information (whether hardcopy or electronic) by including (PA) next to the file series. Additional guidance is contained in DIA Instruction 5015.001, DIA Records Management Program and the DIA Records Management User's Guide.

(b)(3):10 USC 424



4.6. Agency personnel who have Privacy Act questions, concerns, or issues can contact the DIA Privacy Advocate, at [redacted] use the Privacy Act link found at the Directorate for Administration homepage; or contact a member of DIA Privacy Senior Steering Group.

/signed/

[redacted] (b)(3):10 USC 424

Deputy Director for Administration

Enclosures – 3

E1. References

E2. Definitions

E3. Sample Format for System of Records Notice

## E1. Enclosure 1
## References

(f) Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004", 17 December 2004
(g) E-Government Act of 2002, 17 December 2002

## E2. Enclosure 2
## Terms of Reference

**Application** – Software allowing users to execute complex tasks and create and modify documents. Common application types include word processing, spreadsheets, database managers, and graphic presentation programs.

**Confidentiality** – The assurance that Personally Identifiable Information (PII) is not disclosed to unauthorized entities (people and systems).

**Federal Information Security Management Act (FISMA)** of 2002 - Act that provides the framework for securing Federal government information technology, including both unclassified and national security systems.

**Federal Personnel** - Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components). Individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States.

**Federal Register** - The official daily publication for rules, proposed rules and notices of Federal agencies and organizations as well as executive orders and other presidential documents. The Federal Register is published by the Office of the Federal Register, National Archives and Records Administration (NARA).

**Government Contractor -** Personnel employed by private companies and assigned to a contract to accomplish an Agency function, consistent with the Agency's authority. These individuals shall be considered to be employees of the Agency and therefore protected under the Privacy Act.

**Individual** – A U.S. Citizen or alien lawfully admitted for permanent residence.

**Matching program** - Any computerized comparison of automated systems of records described in 5 U.S.C § 552a(a)(8).

**National Security Systems** – An information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon of weapons system, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management (as defined in the Clinger-Cohen Act).

**Network** – A communications medium and all components attached to that medium responsible for the transference of information. Components may include automated information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices. A group of computers and other devices connected to transmission media, usually wire or cable.

**Non-Federal Agency** - Any state or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program.

**Personally Identifiable Information (PII)** – Any personal information collected or maintained by an agency about an individual, other than items of public record, that identifies or can be used to identify, contact or locate the individual.

**Personal Identifier** - A name, identifying symbol, or other identifying particular assigned to an individual for access or identification in a system of records.

**Personal Information** – Information about an individual that identifies, relates, or is unique to, or describes him or her; e.g., a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

**Privacy** – The ability of an individual to exercise control over the collection, use, and dissemination of his or her personally identifiable information.

**Privacy Impact Assessment** – Analysis of how information is handled: (a) to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy, (b) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (c) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Recipient Agency** - Any agency, or employee or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program.

**Record** - Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to his education, financial transactions, medical history, and criminal or employment history, and that contains his name, or the identifying number, symbol or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

**Routine Use** - With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the reason why it was collected.

**Source agency** - Any agency that discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, that discloses records contained in a system of records for use in a matching program.

**Statistical record** - A record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual.

**System** – An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. A set of interrelated components working together to achieve a common purpose.

**System of Records** - A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to the individual.

**US Citizen** – A born or naturalized citizen of the United States.

## E3. Enclosure 3
## System of Records Notice Format

A System of Records Notice published in the Federal Register must include information on the existence and character of the system of records maintained by an agency. The Federal Register is a daily publication that provides a uniform system for publishing Presidential and Federal agency documents. Congress established the Federal Register publication system as a method of informing the public of the regulations affecting them. All System of Records Notices will include the following information:

1. System Name:

2. System Locations:

3. Categories of individuals covered by the system:

4. Categories of records in the system:

5. Authority for maintenance of the system:

6. Purpose:

7. Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

8. Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

9. Storage:

10. Retrievability:

11. Safeguards:

12. Retention and disposal:

13. System Manager(s) and address:

14. Notification procedures:

15. Record access procedures:

16. Contesting records procedures:

17. Record source categories:

18. Exemptions claimed for the system: